Datacryptor ® 2000

FIPS 140-1
Cryptographic Module Security Policy

Racal Security and Payments
www.racalitsec.com

Document History

Part Number	Date	Description
0562a192.001	10 June 1999	Initial version

Distribution List

Text	Location
Master Copy	Project log.

Contents

1 Glossary

3DES	Triple DES
DC2K	Racal Security and Payments Datacryptor 2000 Link encryptor product
DEK	Data Encrypting Key
DES	Data Encryption Standard, a widely used SEA
FIPS	Federal Information Processing Standards
ITSEC	Information Technology Security Evaluation Criteria
KEK	Key Encrypting Key
KV	Key Variable (either a DEK or KEK)
link	Communications link between two DC2K units
SEA	Symmetric Encryption Algorithm
SNMP	Simple Network Management Protocol

2 Related Documents

FIPS 140-1	Federal Information Processing Standards Publication 140-1, 11 January 1994, Security Requirements for Cryptographic Modules

3 Introduction

3.1 Purpose

This document constitutes the security policy for the Datacryptor ® 2000 product hereafter referred to as the DC2K. This document lays down the constraints placed on the operating environment for The DC2K, and then makes security claims for the product, given the proviso of conformance to the delineated environment. These claims are made as a basis for submission to ITSEC evaluation at level E3 and FIPS140-1 validation at level 3.

3.2 Product components

The DC2K product is a secure encryptor supplied as a stand-alone unit. A pair of units may be used to secure a communications link between two host computers.

This is a non-proprietary Cryptographic Module Security Policy for the Datacryptor ® 2000. This policy was prepared as part of FIPS 140-1 certification of the DC2K. FIPS 140-1 (Federal Information Processing Standards Publication 140-1 -- Security Requirements for Cryptographic Modules) gives U.S. Government requirements for cryptographic modules, and defines the Security Policy as:

"A precise specification of the security rules under which the cryptographic module must operate, including rules derived from the security requirements of this standard, and the additional security rules imposed by the manufacturer."

The DC2K provides extraordinary security, meeting all security requirements up to Level 3, and several level 4 requirements. This security policy addresses how the DC2K meets these requirements, and how it can be operated in a secure fashion.

3.3 For more information

This document describes the operations and capabilities of the DC2K in the technical terms of a FIPS 140-1 cryptographic module security policy.

For more detailed information about the DC2K, please visit the Racal Security and Payments web site at http://www.racalitsec.com. The web site contains non-technical descriptions of the Racal Security and Payments products, technical specifications, product offerings, DC2K functionality, DC2K developer information, and more.

For more information about the FIPS 140-1 standard and validation program please visit the NIST web site at http://csrc.nist.gov/cryptval.

For answers to technical or sales related questions please refer to the contacts listed on the DC2K web site at http://www.racalitsec.com.

3.4 Terminology

In this document the Racal Security and Payments Datacryptor ® 2000 is referred to as the DC2K or Datacryptor ®.

4 DC2K Product Overview

The DC2K is an external stand-alone hardware component. Two DC2K units are used to interconnect two networks or computers for secure data communication.

The DC2K encrypts the entire data stream using one of a number of available algorithms, including among others, the Triple DES, DES, and Embattle. Automatic re-synchronization of the cryptographic processes following transmission errors is also performed.

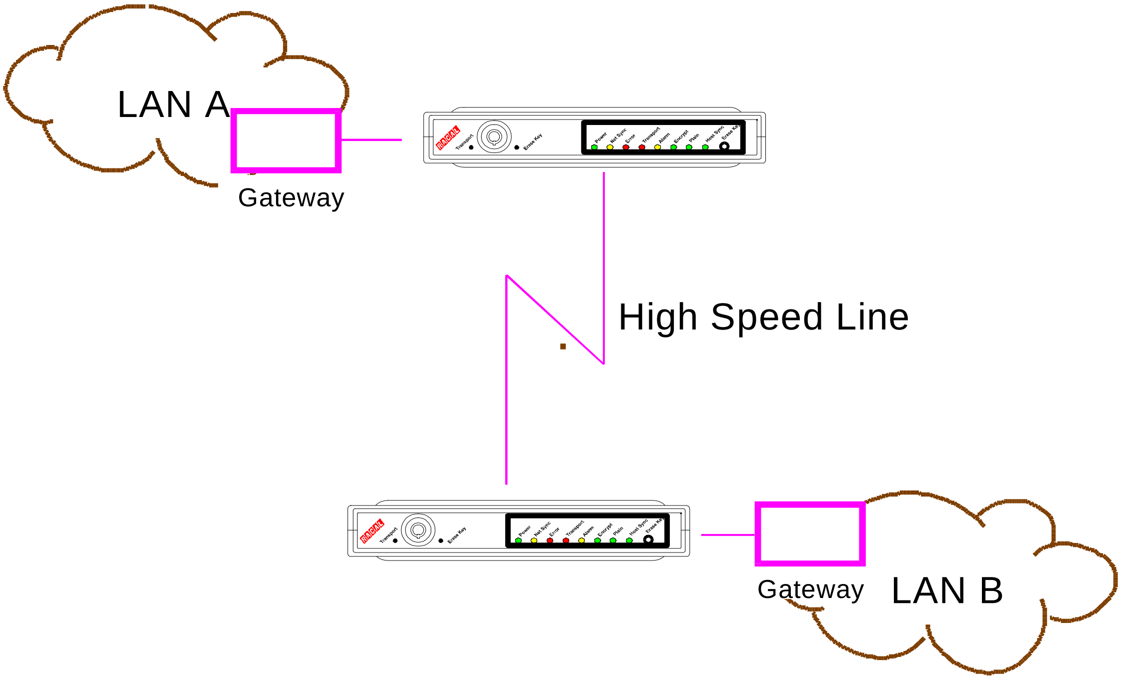

Figure 1 – Example Local Area Network (LAN) implementation of the DC2K to secure data transmission

5 Product rationale

The following subsections identify the security features of the DC2K unit, its purpose, intended environment and method of use. The primary purpose of the DC2K is that of a secure encryptor enforcing data secrecy when data is required to be transmitted from one secure location to another via unsecured public communications networks. All identified threats within such environments are countered either by the unit, or by security procedures that are to be implemented by the user. The perceived threats and the proposed defenses against them are identified below.

5.1 Product features

The DC2K product has a number of variants, including a synchronous link encryptor and a frame relay encryptor. The user and encrypted data may be unframed or framed in accordance with ITU-T recommendation G.704. E1/T1 interfaces are available, as are RS-232 (also known as V.24), X.21 and V.35. The unit has been designed to operate using any suitable software based symmetric encryption algorithm (SEA).

The DC2K unit uses public key technology for key distribution and authentication of all other unit management. The units can be commissioned with their asymmetric key pair securely before being issued to users. Data Encryption Keys (DEKs) are generated internally by the DC2K unit and distributed to a peer DC2K using public key cryptography.

Note: attacks against clear text data before it is passed to the DC2K are beyond the scope of this product.

The communications link between two DC2K units is assumed to be vulnerable and it is the role of the product to protect this zone. In encrypt mode, a unit ensures that data originating at the host port is never transmitted in plain text. In framed modes of communication, it is possible to assign a mode of operation to each time slot, such that each time slot may be assigned to operate in clear, encrypt or standby mode.

The keys and SEA in a DC2K unit are protected using alarm circuitry. If the tamper alarm is triggered, then the keys and SEA loaded in the DC2K unit is erased.

If the DC2K is faulty, as indicated by the failure of a self-test diagnostic, it will revert to its standby mode and will not leave this mode until the fault has been rectified.

6 Key Management

The DC2K and the Element Manager use Digital certificates and the Diffie-Hellman algorithm for the secure commissioning. The secure communication between the Element Manager and a DC2K or two DC2Ks first authenticate with each other based on Certificates and then proceed to use the Diffie-Hellman algorithms for key exchange.

A unit's specific Secret and Public Key is generated during the commissioning process and no one outside of the DC2K knows what is the Secret key value. The Unit's Public key, which is sent to the Element Manager by the DC2K, is used by the Element manager to generate a DC2K specific X.509 certificate. This newly generated certificate is signed by the Universal CA's Secret key. The DC2K's specific Certificate is then sent to the DC2K. It is the newly generated Certificate, which is used to authenticate DC2Ks with each other.

6.1 Key Storage and Protection

The DC2K units generate a Key Encryption Key (KEK) and a Data Encryption KEY (DEK). The KEKs are derived and exchanged between two DC2K using a Diffie-Hellman key agreement.

The DEKs are generated using a FIPS approved Pseudo-Random Number Generator (PRNG). The details of which can be found in FIPS PUB 186-1.

The unit's specific Secret and Public Keys are stored in RAM. The KEKs and DEKs are stored in DRAM. All DC2K keys are destroyed when a DC2K is re-commissioned or attacked.

A DC2K's KEKs and DEKs are destroyed when the unit is attacked, turned on and off or when a new KEK and DEK key exchange takes place.

The secure resin and mesh area of the DC2K protects the DC2K's keys. Any attempt to compromise the unit by removing the DC2K cover or penetrating the DC2K's resin and mesh area, will cause all keys within the unit to be erased.

7 Roles & Services

The DC2K is configured and managed via the Element Manager. Any communication with the DC2K from the Element Manager or from another DC2K is identity based. Signed Certificates are used for authentication between two DC2Ks, or between a DC2K and the Element Manager.

There are two DC2K roles, Crypto-Officer and user. The Crypto-Officer role is used to configure the DC2K via the control port, Ethernet port, or network port.

The user role is when two DC2Ks attempt to establish a secure connection with each other over the Network port. Two DC2Ks will authenticate to one another using digital certificates (CA). This allows the DC2K to meet the requirement for FIPS 140-1 Level 3 security.

The mechanism the DC2K uses for authentication between two or more DC2Ks are defined below.

Identity-Based Authentication

Identity-Based authentication is implemented via Digital Certificates. During the commissioning or administrative process of the DC2K a crypto-officer can download one or multiple digital Certificates to the DC2K. In addition, the crypto-officer can control all Certificate lifetimes.

Transaction Groups

Adding multiple Certificates to a DC2K would allow it to communicate with other DC2Ks that contain at least one of the signed Certificates. This allows for one DC2K to talk with multiple DC2Ks. The DC2K Link operating in framed mode over E1 or T1 is capable of encrypting traffic from a different DC2K on each of its available timeslots.

The Frame Relay (multi-channel) DC2K is capable of talking with multiple DC2K over separate channels.

7.1 Crypto-Officer Role and Services Available

The only user that the DC2K Datacryptor ® Element Manager is allowed to authenticate based on identity is the Crypto-Officer. The Crypto-Officer will have the following services available:

1. Login to the DC2K using identity based authentication.

2. Logout of the DC2K
3. Commission the DC2K with a Certificate of Authority (CA).
4. Change CA on a DC2K.
5. Adding multiple Certificates (creating a transaction group) to a DC2K
6. Enable/Disable motion and temperature alarms.
7. Install different security software modules such as DES, CA, and Diffie-Hellman parameters on the DC2K.
8. Modify the Key Encryption Key change interval.
9. Modify the Data Encryption Key change interval.
10. Configure additional DC2Ks
11. Cloning a particular DC2K
12. Deleting a DC2K unit
13. Restoring a DC2K unit
14. Configure a DC2Ks IP address, connection method or unit name.

For detailed information on the services available to the Crypto-Officer, please refer to the DC2K Element Manager manual.

It is possible to monitor the state of a DC2K remotely using either the Element Manager software or SNMP software. State monitoring is a non-authenticated function of the DC2K.

7.2 User Role and Services Available.

- The user role is considered as two DC2Ks communicating with each other in a transaction Group. Again, digital Certificates loaded into each DC2K is used as the mechanism for identity-based authentication.

8 Secure Operation of the DC2K

The secure operation of the DC2K consists of the initial commissioning of the unit and later administrative procedures.

Note that an identity based authentication scheme using Certificates is used whenever the crypto-officer administers a DC2K. Identity based authentication using signed Certificates also applies to two DC2Ks communicating with each other.

8.1 Management Options

The DC2K can be managed using several methods. These methods are:

1. Datacryptor ® Element Manager- This software allows a Crypto Officer to administer the DC2K as described in Section 6.

2. SNMP management Station – This is limited to requesting and obtaining status information from the Datacryptor.

Note: Only one management session is allowed at any one time

9 FIPS 140-1 Mode of Operation

FIPS 140-1 mode of operation is defined as a mode in which only FIPS allowed or approved security methods are used.

Examples of FIPS approved/allowed security methods are:

- DES
- 3DES
- DSA
- SHA-1
- Diffie-Hellman (Allowed method while in FIPS mode)

By default, the DC2K has the 3DES, DSA, SHA-1, and Diffie-Hellman algorithms preloaded in the factory. In addition, the Racal Certificate Authority is also preloaded.

Having the DC2K operate under these conditions will place the DC2K in FIPS 140-1 mode. Note that only one encryption algorithm such as 3DES or DES can be loaded into the unit at any one time.

9.1.1 Other Encryption Algorithms

As previously stated, the DC2K comes preloaded with the 3DES algorithm. A customer can request a different encryption algorithm such as DES from Racal Security and Payments. At that point, Racal will issue a new firmware file that contains the new encryption algorithm. The customer will then need to download the new firmware file to the DC2K. Note that all firmware files are digitally signed by the Racal Manufacturing CA and verified by the DC2K when downloaded.

Note: Firmware files may not be useable in a FIPS 140 mode of operation unless it has been validated to FIPS 140-1 security requirements. This is true even if the firmware files contain FIPS approved algorithms.

9.2 FIPS 140-1 Level 3 Security Mode of Operation.

For Level 3 Security, the following must be met.

1. Use of the FIPS approved/allowed algorithms listed previously.
2. Enabling motion detection on the DC2K
3. Enabling Diffie-Hellman Key Distribution each time the Data Encryption Keys (DEK) changes.

NOTE

The DC2K uses the Diffie-Hellman algorithm for the Key Encryption Key (KEK) and Data Encryption Key (DEK), Key Distribution. The KEK is used to encrypt the DEK and exchange the DEKs that is generated at each DC2K unit. There is a DC2K option to update the KEK with the DEK. For FIPS 140-1 mode of operation, KEK must be updated each time the DEK is also updated. Essentially, the Diffie-Hellman algorithm is used whenever there is a DEK exchange between units.

10 Threats to the system

10.1 Operational Vulnerabilities

In order to provide adequate security, the unit needs to be used in association with a set of security procedures. The following section identifies possible vulnerabilities in operation and identifies the Security procedures used to address them.

10.1.1 Commissioning of DC2K units

While commissioning a DC2K the secret key of the Certificate Authority is at risk of disclosure. In systems where the secret keys are pre-generated, they are at risk from point of generation to when they are installed in the DC2K. To counter act this vulnerability, all keys should be securely stored and transported.

10.1.2 Host link security

The connection between the Element Manager and the Host port of the DC2K is authenticated during and after the commissioning process. Essentially, any communication between the Element Manager and the DC2K is identical to the Key Management and authentication mechanism of two DC2Ks.

10.1.3 Secure location of equipment

If the DC2K is used in a FIPS 140-1 compliant mode, the Datacryptor ® will erase keys and algorithms if moved. The enabling of the motion sensor of the DC2K can prevent an unauthorized person from moving the DC2K unit to a new location without the alarm triggering and zeroing the DC2K unit of keys and encryption algorithms.

10.1.4 Encrypt Mode Only

The Crypto-Officer can place the DC2K unit in either Plain Text mode or Encrypt mode. In either case, LEDs in the front panel of the unit or the Element Manager will indicate the security mode the unit is operating under. In this way, the Crypto-Officer will know of the unit is operating in Plain Text mode or Encrypt Mode.